WHAT IS CLAIMED IS:

1. A method of communicating data securely within a wireless communications network, comprising the steps of:

receiving a first authentication request from a mobile station;

providing a first key to said mobile station in response to said authentication;

receiving a second authentication request from a database server, said second authentication request further including said first key provided by said mobile station and a particular database record to which said mobile station is requesting access;

determining whether said mobile station has authority to access said particular database record; and

in response to said affirmative determination,

instructing said database server to provide information associated with said requested database record to said mobile station wherein said information is encrypted; and

providing said mobile station with a second key enabling said mobile station to decrypt said information received from said database server using said second key.

2. The method of Claim 1 wherein said step of providing said first key to said mobile station further comprises the step of providing a time out period for said first key to said mobile station.

3. The method of Claim 1 wherein said information stored in said database server is encrypted using a data access key and said second key is generated from said data access key and said first key.

4. The method of Claim 1 wherein said step of instructing said database server to provide information to said mobile station further comprises the step of providing said database server with a third key wherein said third key is used by said database server to further encrypt said information.

5. The method of Claim 4 wherein said information stored in said database server is encrypted using a data access key and wherein said third key is generated from said data access key and said first key and said second key is generated from said data access key, said first key and said third key.

6. The method of Claim 1 further comprising the steps of:

receiving a third authentication request from said database server requesting authorization to update said particular database record by said mobile station;

determining whether said mobile station has authority to update said database record; and

in response to an affirmative determination,

instructing said database server to allow said mobile station to update information associated with said database record; and

providing said mobile station with said second key enabling said mobile station to encrypt any information to be transmitted over to the database server to be updated at said database record.

7. The method of Claim 1 wherein said information stored in said database record is encrypted using a data access key and said second key provided to said mobile station is generated from said data access key and said first key.

8. The method of storing and communicating data securely within a mobile telecommunications network wherein said mobile telecommunications network provides wireless service to a wireless device and further includes a mobile authentication server, comprising the steps of:

storing particular information within a database server wherein said data is stored encrypted using a first encryption key;

receiving a request from said wireless device to access said information within said database server;

in response to said request, transmitting a authentication request from said database server to said mobile authentication server;

receiving authentication approval from said authentication server regarding said wireless device for said requested information; and

providing said requested information to said wireless device without decrypting said information.

9. The method of Claim 8 wherein said step of receiving said authentication approval from said authentication server further comprises the steps of:

receiving a second encryption key from said authentication server;

encrypting said stored information using said second encryption key; and

providing said encrypted information to said wireless device.

10. The method of Claim 8 wherein said step of receiving said request from said wireless device to access said information further comprises the step of receiving a session key generated by said authentication server from said wireless device.

11. The method of Claim 10 wherein said step of transmitting said request to said authentication server further comprises the step of including said session key within said request.

12. The method of Claim 8 further comprising the steps of:

receiving a second request from said wireless device to store particular information within said database server;

transmitting a second authentication request to said authentication server;

receiving second authentication approval from said authentication server instructing said database server to allow said wireless device to update said database server with said requested information;

receiving said particular information from said wireless device wherein said information being encrypted using a particular encryption key; and

storing said encrypted information within said database server.

13. An authentication server for communicating data securely within a wireless communications network providing wireless service to a wireless device and communicatable within a database server associated within a data communications network, comprising:

a session key generator for generating a particular session key to be used by said wireless device in response to said wireless device registering with said authentication server;

a database record for correlating a particular database record with a particular first encryption key;

wherein said database record further correlating identities of authorized users with said particular database record;

an encryption key generator for generating a second encryption key to be provided to said wireless device for decrypting certain information associated with said database record stored within said database server.

14. The authentication server of Claim 13 further comprising a clock module for assigning a time period for said session key generated for said wireless device for said assigned time period.

15. The authentication server of Claim 13 wherein said encryption key generator generates said second encryption key from said session key and said first encryption key.

16. The authentication server of Claim 13 further comprises an interface module for receiving an authentication request from said database server wherein said authentication request further includes said session key associated with said wireless device and particular database record to which said mobile device requested access.

17. The authentication server of Claim 16 further comprising a second encryption key generator for generating a third encryption key to be provided to said database server in response to said authentication request wherein said third encryption key used by said database server for further encrypting said information stored within said database server associated with said requested database record.

18. The authentication server of Claim 17 wherein said encryption key generator generates said second encryption key from said session key, said first encryption key and said third encryption key.

19. A database server for storing and communicating data securely with a wireless device associated within a mobile communications network, said mobile communications network including a mobile authentication server, comprising:

means for storing particular information within said database server wherein said data is stored encrypted using a first encryption key;

means for receiving a request from said wireless device to access said stored information within said database server;

means for transmitting an authentication request to said mobile authentication server in response to said request;

means for receiving authentication approval from said authentication server regarding said wireless device for said requested information; and

means for providing said requested information to said wireless device without decrypting said information.

20. The database server of claim 19 wherein said means for receiving said authentication approval from said authentication server further comprises:

means for receiving a second encryption key from said authentication server;

means for encrypting said stored information using said second encryption key; and

means for providing said encrypted information to said wireless device.

21. The database server of Claim 19 wherein said request from said wireless device to access said information further comprises a session key generated by said authentication server from said wireless device.

22. The database server of Claim 21 wherein said request to said authentication server further comprises said session key received from said wireless device.